PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : G05B 19/042

A1

(11) Internationale Veröffentlichungsnummer: **WO 98/40796**

(43) Internationales Veröffentlichungsdatum: 17. September 1998 (17.09.98)

(21) Internationales Aktenzeichen: PCT/DE98/00633

(22) Internationales Anmeldedatum: 3. März 1998 (03.03.98)

(30) Prioritätsdaten:
197 09 956.4 11. März 1997 (11.03.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D-80333 München (DE).

(72) Erfinder; und

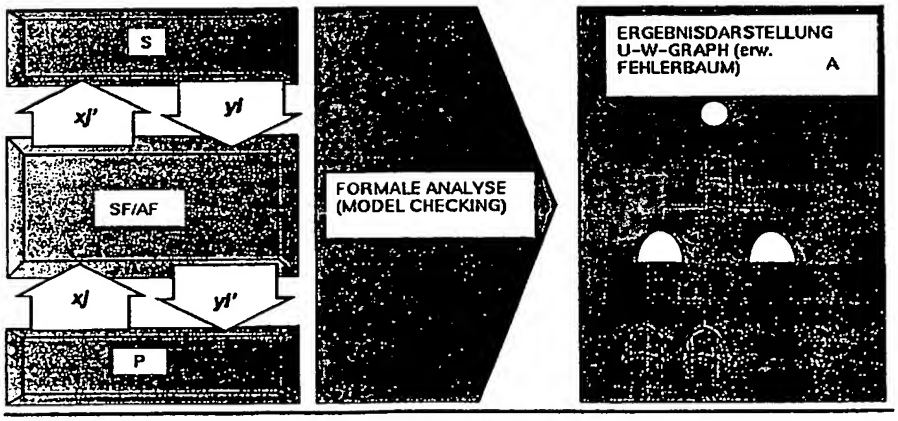
(75) Erfinder/Anmelder *(nur für US)*: LIGGESMEYER, Peter [DE/DE]; Hauptstrasse 89, D-85579 Neubiberg (DE).

(81) Bestimmungsstaaten: US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD FOR COMPUTER-ASSISTED ERROR CHECKING OF SENSORS AND/OR ACTORS IN TECHNICAL SYSTEMS

(54) Bezeichnung: VERFAHREN ZUR RECHNERGESTÜTZTEN FEHLERANALYSE VON SENSOREN UND/ODER AKTOREN IN EINEM TECHNISCHEN SYSTEM



A... REPRESENTATION U-W GRAPH (EXT. ERROR TREE)

(57) **Abstract**

Disclosed is a method wherein a state description of the technical system for an error occurrence and a state description of the technical system for error-free operation is determined in order to detect sensor and/or actor errors. The attainable states for both descriptions are preferably determined by model checking. A varying number of states of both descriptions is formed, said states being checked as to whether they comply with predeterminable conditions (e.g. safety requirements).

(57) Zusammenfassung

Es wird ein Verfahren vorgeschlagen, bei dem für einen Fehler eines Sensors und/oder eines Aktors eine zustandsendliche Beschreibung des technischen Systems für den Fehlerfall und eine zustandsendliche Beschreibung des technischen Systems für den fehlerfreien Fall ermittelt wird. Für beide Beschreibungen werden jeweils die erreichbaren Zustände vorzugsweise mittels Model Checking ermittelt. Es wird eine Differenzmenge von Zuständen der beiden Beschreibungen gebildet, für deren Zustände überprüft wird, ob diese Zustände vorgebbaren Bedingungen genügen (z.B. Sicherheitsbedingungen).

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Beschreibung

Verfahren zur rechnergestützten Fehleranalyse von Sensoren und/oder Aktoren in einem technischen System

Für komplexe technische Systeme oder Anlagen ist es von enormer Bedeutung, Aussagen über die Zuverlässigkeit des jeweiligen Systems bzw. der Anlage treffen zu können.

Es ist bekannt, daß Aussagen über die Zuverlässigkeit eines beliebigen technischen Systems bzw. einer Anlage manuell, beispielsweise durch eine sog. Fehlerbaumanalyse (vgl. [1]), oder simulativ bzw. analytisch auf Basis von speziell zu diesem Zweck erstellten Modellen (vgl. [2]) erzeugt werden können. Zur einfacheren Darstellung wird im weiteren nur noch von technischen Systemen gesprochen. Technische Anlagen sind im Rahmen dieses Dokuments jedoch in dem Begriff des technischen Systems umfaßt. Eine vollständige manuelle Ermittlung der Auswirkungen eines technischen Fehlverhaltens von Sensoren und/oder Aktoren, ist in einem komplexen technischen System aufgrund der vernetzten Abhängigkeiten und der unterschiedlichen Realisierungsformen der Steuerung, des gesteuerten Systems und der Sensorik und/oder Aktorik praktisch nicht möglich. Die in [2] beschriebenen analytischen Techniken erfordern die Erstellung eines speziellen Modells, für das im allgemeinen nicht garantiert werden kann, daß es das jeweils betrachtete System korrekt beschreibt. Dadurch wird natürlich die Qualität der Aussagen erheblich reduziert. Ferner ist ein erheblicher Nachteil der in [2] beschriebenen Ansätze, daß die Modellerstellung zusätzlichen Entwicklungsaufwand und Zeit erfordert. Dadurch wird eine kurzfristige Untersuchung alternativer Realisierungen eines technischen Systems, was auch als Rapid Prototyping bezeichnet wird, verhindert.

Es ist bekannt, ein technisches System in einer zustandsendlichen Beschreibung, z.B. als Automat, zu beschreiben. Eine zustandsendliche Beschreibung weist üblicherweise Zustände

auf, in denen Aktionen durchgeführt werden, wenn sich das technische System in dem jeweiligen Zustand befindet. Ferner weist die zustandsendliche Beschreibung üblicherweise Zustandsübergänge auf, die mögliche Wechsel des technischen Systems zwischen Zuständen beschreiben. Auch bei Zustandsübergängen kann das technische System Aktionen durchführen. In einem gesteuerten technischen System ist es in diesem Zusammenhang bekannt, die zustandsendliche Beschreibung derart auszugestalten, daß das Verhalten der Steuerung des technischen Systems und das Verhalten der gesteuerten Anlage als Zustandsautomat dargestellt wird. Auch ist bei diesen Ansätzen nicht sichergestellt, daß alle möglichen Fehlerauswirkungen auf das System korrekt ermittelt werden.

Möglichkeiten zur textuellen Beschreibung eines Zustandsautomaten, die mit einem Rechner verarbeitet wird, sind z.B. Interlocking Specification Language (ISL) oder Control Specification Language (CSL), die in [3] beschrieben sind.

Es ist ferner bekannt, eine zustandsendliche Beschreibung für die Generierung von Steuerungen durch einen Rechner und für den rechnergestützten Nachweis von Eigenschaften eines fehlerfreien technischen Systems zu verwenden.

Eine Möglichkeit zum rechnergestützten Nachweis von Eigenschaften eines fehlerfreien technischen Systems verwendet das Prinzip des sog. Model Checkings, das in [4] beschrieben ist.

Ferner ist es bekannt zur zustandsendlichen Beschreibung eines Systems ein sogenanntes Finite State Machine-Format (FSM-Format) zu verwenden, deren Grundlagen in [5] beschrieben sind. Binary Decision Diagrams (BDD) besitzen den Vorteil, in vielen Fällen auch sehr umfangreiche Zustandssysteme kompakt zu repräsentieren.

Somit liegt der Erfindung das Problem zugrunde, ein Verfahren zur rechnergestützten Fehleranalyse von Sensoren und/oder Ak-

toren in einem technischen System anzugeben, mit dem die Korrektheit der Fehleranalyse gewährleistet wird.

Das Problem wird durch das Verfahren mit den Merkmalen des Patentanspruchs 1 gelöst.

Das Verfahren wird mit einem Rechner durchgeführt und umfaßt folgende Schritte:

a) für einen Fehler eines Sensors und/oder eines Aktors des Systems wird eine zustandsendliche Beschreibung des technischen Systems für den Fehlerfall ermittelt,

b) für das technische System wird eine erste Menge erreichbarer Zustände ermittelt,

c) für das fehlerbehaftete technische System wird eine zweite Menge erreichbarer Zustände ermittelt,

d) es wird eine Differenzmenge aus der ersten Menge und der zweiten Menge gebildet,

e) es werden Ergebniszustände aus der Differenzmenge ermittelt, die vorgebbaren Bedingungen genügen.

Anschaulich kann die Erfindung dadurch beschrieben werden, daß ein Model Checking sowohl für das fehlerfreie technische System als auch ein mit einem Fehler eines Sensors und/oder Aktors behafteten System durchgeführt wird. Durch das Model Checking werden alle erreichbaren Zustände des fehlerfreien bzw. des fehlerbehafteten Systems ermittelt. Aus diesen Zuständen wird eine Differenzmenge von Zuständen gebildet. Für die Differenzmenge werden die Zustände der Differenzmenge ermittelt, die einer vorgebbaren Bedingung genügen, z.B. einer Sicherheitsanforderung an das System. Diese Zustände stellen für den jeweils untersuchten Fehlerfall einen „gefährlichen" Zustand bzgl. der vorgebbaren Bedingung dar.

Durch das Verfahren wird gewährleistet, daß alle für den jeweils untersuchten Fehlerfall, d.h. für den fehlerhaften Sensor und/oder Aktor, hinsichtlich vorgebbarer Bedingungen „gefährliche" Zustände ermittelt werden.

Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Es ist vorteilhaft, das Verfahren für alle möglichen Fehler von Sensoren und/oder Aktoren, die das technische System aufweist, durchzuführen. Auf diese Weise wird für das gesamte System gewährleistet, daß hinsichtlich vorgebbarer Bedingungen alle „gefährlichen" Zustände ermittelt werden.

Ferner ist es vorteilhaft, den Sensoren und/oder Aktoren Ausfallwahrscheinlichkeiten zuzuordnen und die Fehleranalyse unter Berücksichtigung der Ausfallwahrscheinlichkeiten durchzuführen. Auf diese Weise wird es ohne größeren Rechenaufwand bei der Durchführung des Verfahrens mit einem Rechner möglich, für die ermittelten Zustände anzugeben, mit welcher Wahrscheinlichkeit dieser Zustand tatsächlich erreicht wird, womit eine Risikoabschätzung für das jeweils analysierte System sehr einfach und anschaulich möglich wird.

Weiterhin ist es zur weiteren Rechenzeiteinsparung bei der Durchführung des Verfahrens mit einem Rechner vorteilhaft, die zustandsendliche Beschreibung durch einen endlichen Automaten in Form eines Binary Decision Diagrams (BDD) zu realisieren.

Das Verfahren kann durch die oben Beschriebenen Eigenschaften sehr vorteilhaft in folgenden Gebieten Verwendung finden:
- beim Rapid Prototyping des technischen Systems.
- im Rahmen der Fehlerdiagnose des technischen Systems.
- zur Generierung kritischer Prüffälle für eine Inbetriebsetzung und einen Systemtest des technischen Systems.
- zur präventiven Wartung des technischen Systems.

In den Figuren ist ein Ausführungsbeispiel der Erfindung dargestellt, welches im weiteren näher erläutert wird.

Es zeigen

Figur 1 ein skizzenhafte Darstellung des Verfahrens;

Figur 2 eine Skizze einer zustandsendlichen Beschreibung einer Steuerung und des durch die Steuerung gesteuerten Prozesses eines technischen Systems, wobei die fehlerfreie Steuerung und der Prozeß jeweils als ein eigener Zustandsautomat beschrieben sind;

Figur 3 eine Skizze der zustandsendlichen Beschreibung aus Figur 1 mit einem symbolisch dargestellten allgemeinen Sensorfehlermodell und Aktorfehlermodell;

Figur 4 eine Skizze der zustandsendlichen Beschreibung aus Figur 1 mit einem symbolisch dargestellten nichtpersistenten Fehler eines Sensors;

Figur 5 eine Skizze der zustandsendlichen Beschreibung aus Figur 1 mit dem Fehler aus Figur 4, wobei als Ersatz des Fehlermodells die Steuerung modifiziert wurde;

Figur 6 eine Skizze einer Draufsicht des Ausführungsbeispiels, einem Hubdrehtisch einer Fertigungszelle;

Figur 7 eine Skizze, in der die vorgesehene Bewegung des Hubdrehtischs aus Figur 6 dargestellt ist;

Figur 8 eine Skizze des Zustandsraums des fehlerfreien Hubdrehtischs;

Figur 9 eine Skizze des Zustandsraums eines fehlerbehafteten Hubdrehtisch;

Eine geeignete zustandsendliche Beschreibung stellt das Verhalten der Steuerung und das Verhalten der gesteuerten Anlage als Zustandsautomat dar. Die Darstellung kann auf unterschiedliche Weise, z.B. in textueller Form unter Verwendung von ISL oder CSL, erfolgen.

In Figur 2 ist ein einfaches technisches System mit einer fehlerfreien Steuerung FS, Zuständen y1, y2, y3 und Zustandsübergängen x1, x2 als Zustandsautomat dargestellt. Die Steuerung S beschreibt als Zustände Aktoren. Ein gesteuerter

Prozeß P enthält die Beschreibung von Sensoren x1, x2, x3 als Zustände x1, x2, x3 und Zustandsübergänge y1, y2, y3.

Die Steuerung S des Systems reagiert auf Meßwerte xj(x1, x2, x3) von Sensoren X.Somit werden durch Sensordaten daher in der Steuerung S Zustandsübergänge ausgelöst. Die Zustände sind durch Werte yi (y1, y2, y3) von Zustandsvariablen Y charakterisiert, die Aktoren zugeordnet sind. Das Stellen von Aktoren Y löst wiederum Zustandsübergänge in der gesteuerten Anlage, d.h. in dem Prozeß P aus, was sich in einer Modifikation der Werte der Sensoren X äußert.

Die Zustandsautomaten der Steuerung S und des Prozesses P führen alternierend Zustandsübergänge durch. Die Ausgaben des einen Automaten sind die Eingaben des jeweils anderen Automaten.

Die Schnittstelle zwischen Steuerung und gesteuerter Umgebung kann in einer entsprechenden Beschreibung automatisch erkannt werden. Ferner ist es möglich, wie im weiterem detailliert beschrieben wird, einer derartigen Beschreibung den Wertevorrat zu entnehmen, den die einzelnen Werte (Zustände bzw. Zustandsübergänge) annehmen können.

In Figur 3 ist symbolisch eine Fehlermodellierung für fehlerhafte Sensoren in einem Sensorfehlermodell SF und für fehlerhafte Aktoren in einem Aktorfehlermodell AF dargestellt.

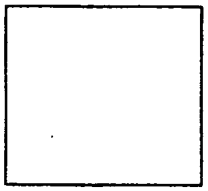
Technisch sind also an der Schnittstelle zwischen Steuerung S und gesteuertem Prozeß P Sensoren X und Aktoren Y angeschlossen. Ein Fehlverhalten eines Sensors X führt dazu, daß anstelle des korrekten Meßwerts x_j ein anderer, fehlerhafter Wert x_j' an die Steuerung S geliefert wird, d.h. der Steuerung S zugeführt wird. Ein Fehlverhalten eines Aktors äußert sich im Einstellen eines falschen Werts y_i' anstelle des Werts yi. Welche Sensoren X und Aktoren Y vorhanden sind und

welcher Wertevorrat hier zu berücksichtigen ist, kann der zustandsendlichen Beschreibung entnommen werden.

Dies gestattet die automatisierte, systematische Analyse der Auswirkungen von Sensor- und Aktorfehlern auf das Verhalten eines gesteuerten Systems. Zwischen den gesteuerten Prozeß P und die Steuerung S werden Sensorfehlermodelle SF bzw. Aktorfehlermodelle AF geschaltet, die den jeweiligen Fehler des Sensors x und/oder Aktors y beschreiben. In der Figur 3 sind beispielhaft Modelle für intermittierende (nicht persistente) Einzelfehler der Sensorik und Aktorik angegeben.

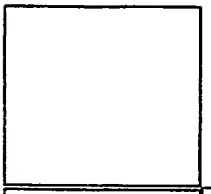
Ein nichtpersistenter Einzelfehler eines Sensors x wird beschrieben durch folgende Vorschrift:

$x'_j = x_j \mid j \neq n$ (fehlerfreie Werte)

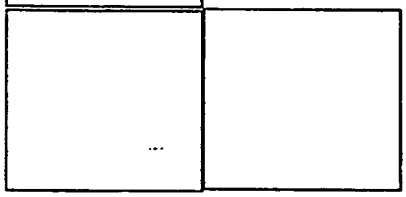


(fehlerhafter Wert).

Ein nichtpersistenter Einzelfehler eines Aktors y wird beschrieben durch folgende Vorschrift:



(fehlerfreie Werte)



(fehlerhafter Wert).

Figur 4 zeigt das allgemeine Sensorfehlermodell SF aus Figur 3 für den Fall, daß ein nichtpersistenter Einzelfehler bei einem ersten Sensorwert x1 vorliegt derart, daß der erste Sensorwert x1 entweder den korrekten ersten Sensorwert x1 oder aufgrund eines Sensorfehlers einen zweiten Sensorwert x2

aufweist, der in diesem Fall ein fehlerhafter Wert wäre. Der zweite Sensorwert x2 und ein dritter Sensorwert x3 werden korrekt gemessen.

Eine wichtige Frage, die es zu beantworten gilt, ist nun, ob die Kombination aus Steuerung S und gesteuerten Prozeß P aufgrund des Sensorfehlers in kritische Zustände gelangen kann, die im fehlerfreien Fall sicher ausgeschlossen werden konnten.

Eine Möglichkeit, diesen Nachweis für den fehlerfreien Fall zu erbringen, bietet das sogenannte Model Checking, welches in [4] beschrieben ist. Dieses Verfahren gestattet es, die Menge der erreichbaren Zustände zu ermitteln und zu untersuchen, ob Zustände enthalten sind, die z.B. Sicherheitsbedingungen verletzen.

Um diese Technik zur Fehleranalyse von in dem System enthaltenen Sensoren X und/oder Aktoren Y anwenden zu können, werden hier die Sensorfehlermodelle SF bzw. Aktorfehlermodelle AF durch eine geänderte Steuerungslogik beschrieben (vgl. Figur 5).

Die in Figur 5 dargestellte Kombination aus Steuerung S und gesteuertem Prozeß P verhält sich identisch zu dem in Figur 4 dargestellten Modell für den Fehlerfall bei dem ersten Sensorwert x1. Es kann hier jedoch auf den Einschub eines expliziten Fehlermodells zwischen Steuerung S und gesteuertem Prozeß P verzichtet werden. Aufgrund des angenommenen intermittierenden Fehlers werden in der Steuerung mit x1 indizierte Zustandsübergänge parallel zu den mit x2 markierten Zustandsübergängen hinzugefügt.

Damit wird der folgende Sachverhalt beschrieben:
Der zweite Sensorwert x2 und der dritte Sensorwert x3 werden korrekt gemessen. Daher ist das Steuerungsverhalten für diese Werte unmodifiziert. Da ein intermittierender Fehler angenom-

men wird, kann auch der erste Sensorwert x1 korrekt gemeldet werden, so daß diese Zustandsübergänge erhalten bleiben. Würde eine persistente Vertauschung von dem ersten Sensorwert x1 mit dem zweiten Sensorwert x2 angenommen, so müßten mit x1 beschriftete Kanten gelöscht werden. Alle Zustandsübergänge die mit x2 markiert sind, können nun auch beim Wert x1 durchlaufen werden. Daher wird eine entsprechende Kante in der Steuerung S ergänzt. Die Steuerung S reagiert auf den Wert x2, aber an der Stelle x1 des Prozesses.

Diese Modifikation der Steuerungslogik zur Beschreibung von Fehlern kann formal für alle betrachtbaren Fehler automatisch durch den Rechner durchgeführt werden.

Für die entstehenden Modelle können die Fragen nach der Erreichbarkeit von kritischen Zuständen (z.B. Sicherheit, Verklemmungen) ebenfalls durch Anwendung des Model Checkings beantwortet werden. Es erfolgt also eine automatische Ermittlung der im fehlerbehafteten System erreichbaren Zustände vorzugsweise unter Verwendung des Model Checkings.

Anschließend wird jeweils eine Differenzmenge der im jeweiligen Fehlerfall erreichbaren Zustände und der im fehlerfreien Fall erreichbaren Zustände ermittelt.

Aus der Differenzmenge werden jene Zustände ermittelt, die mindestens einer vom Benutzer vorgebbaren Bedingung (z.B. Verletzung einer Sicherheitsanforderung) genügen bzw. diese verletzen, je nach Anwendung.

In Figur 1 ist diese Vorgehensweise noch einmal in einem Blockschaltbild symbolisch dargestellt. Für die Steuerung FS und den gesteuerten Prozeß P wird mindestens ein Sensorfehlermodell SF und/oder mindestens ein Aktorfehlermodell AF erstellt, unter deren Berücksichtigung eine formale Analyse der zustandsendlichen Beschreibung für das fehlerbehaftete System vorzugsweise durch Model Checking erfolgt.

Für das Ergebnis des Vergleichs mit dem fehlerfreien System und der Ermittlung „gefährlicher" Zustände werden die Ursache-Wirkungs-Zusammenhänge zwischen Sensor- bzw. Aktorfehlern und dem möglichen Eintritt der betrachteten Wirkung ermittelt und vorzugsweise in einem Ursache-Wirkungs-Graph dargestellt.

In Figur 6 ist ein technisches System in Form eines Hubdrehtischs HD einer Fertigungszelle FZ dargestellt, mit dem das Verfahren noch detaillierter dargestellt werden soll.

Die Fertigungszelle FZ weist ein zuführendes Förderband FB, an dessen Ende ein Hubdrehtisch Werkstücke WS aufnimmt und einem Roboter R zuführt. Der Roboter R legt das Werkstück WS in eine Presse PR und gibt es nach dem Formen auf ein wegführendes Band WB. Die Fertigungszelle FZ enthält entsprechende Sensoren X und Aktoren Y.

Der Hubdrehtisch HD kann sich mit Hilfe zweier Antriebe (nicht dargestellt) in vertikaler (vmov) und horizontaler (hmov) Richtung bewegen. Jeder Antrieb kann in negative (minus) oder positive (plus) Richtung angesteuert werden oder stillstehen (stop).

Der Hubdrehtisch HD verfügt über Sensoren X zur vertikalen (vpos) und horizontalen (hpos) Positionserfassung, die die Positionen x0 (unten), x1 (mitte) und x2 (oben) unterscheiden können. Zusätzlich erfaßt ein weiterer Sensor (part_on_table) (nicht dargestellt) das Vorhandensein eines Werkstücks WS auf dem Hubdrehtisch HD.

Die Ausgangsposition AP des Hubdrehtischs HD ist am unteren, linken Anschlag (x0,x0) ohne Werkstück WS (vgl. Figur 7). Falls ein Werkstück WS vom zuführenden Förderband FB auf den Hubdrehtisch HD fällt, so ist die Zielposition ZP des Hubdrehtischs HD oben rechts (x2, x2).

Der Hubdrehtisch HD darf niemals eine andere horizontale Position als x0 (linker Anschlag) in Kombination mit der vertikalen Position x0 (unten) einnehmen, da er sonst mit dem zuführenden Förderband FB kollidieren würde (verbotener Bereich VB).

Im weiteren ist eine Beschreibung des Zustandsautomaten der Steuerung FS des Hubdrehtischs HD in CSL angegeben:

```
CSLxtClasses table
  Types
       bool          = [nein, ja];
       posType       = [x0, x1, x2];
       movType       = [stop, plus, minus] ;

Class pcd

StateVariables
     input  vpos            : posType default x0;
     input  hpos            : posType default x0;
     input  part_on_table   : bool    default nein;
     output vmov: movType default stop;
     output hmov: movType default stop;

Transitions
start_up  :=  (part_on_table = ja /\ vpos = x0)
          ==> (** vmov = plus);
rotate    :=  (part_on_table = ja /\ vpos = x1 /\ hpos < x2)
          ==> (** hmov = plus);
stophigh  :=  (part_on_table = ja /\ vpos = x2)
          ==> (** vmov = stop);
stop45    :=  (part_on_table = ja /\ hpos = x2)
          ==> (** hmov = stop);
rotate_back    := (part_on_table = nein /\ vpos = x2 /\
          /\ hpos = x2) ==> (** hmov = minus);
start_down     :=  (part_on_table = nein /\ hpos = x0 /\
          /\ vpos = x2) ==> (** hmov = stop /\
```

```
            /\ ** vmov = minus);
stoplow     :=  (part_on_table = nein /\ vpos = x0)
            ==> (** vmov = stop);

  End /* Class pcd_controll*/
End table
CSLInstances i
     table : pcd;
End i
```

Die oben angegebene Beschreibung in CSL legt die Steuerungslogik des Hubdrehtischs HD fest. Der Kopf der CSL-Beschreibung vereinbart Datentypen (Wertebereiche) der Zustandsvariablen. Die anschließende Deklaration der Zustandsvariablen nutzt diese Typvereinbarungen und legt zusätzlich Anfangswerte fest. Anhand der Vereinbarung von Zustandsvariablen als Input oder Output kann festgestellt werden, ob es sich um eine Zustandsvariable handelt, die den Prozeßzustand darstellt oder ob sie Zustände der Steuerung FS kodiert. Inputvariablen der Steuerung FS kodieren Prozeßzustände. Outputvariablen der Steuerung FS kodieren Steuerungszustände. Die Zeile „input vpos: posType default x0" deklariert eine Zustandsvariable mit Namen „vpos", die die Werte x0, x1 *und* x2 (die Werte des Typs posType) annehmen kann und deren Anfangswert x0 ist.

Die Transitionen (Transitions) dienen zur Beschreibung der Steuerungslogik. Transitionen werden ausgelöst durch Wertekombinationen der Inputvariablen der Steuerung FS, die Prozeßzustände darstellen - also die Position des Hubdrehtischs HD in der vertikalen (vpos) und der horizontalen (hpos) Bewegungsrichtung und das Vorhandensein eines Werkstücks WS auf dem Hubdrehtisch HD (part_on_table). Die Werte der Outputvariablen vmov und hmov werden durch die Transitionen, die die Steuerungslogik implementieren, modifiziert. Sie beschreiben die Zustände der Steuerung. Ihre Werte werden allein durch

Zustandsübergänge der Steuerung, also durch die der Steuerung eingeprägte Logik modifiziert.

Diese Informationen können aus der CSL-Beschreibung automatisch entnommen werden. Es kann zwischen Eingaben der Steuerung (Inputs, Sensordaten) und Ausgaben der Steuerung (Outputs: Aktorkommandos) unterschieden werden. Außerdem sind die jeweils möglichen Werte erkennbar (Typdeklarationen).

Die Informationen bleiben im wesentlichen auch nach der Übersetzung der CSL-Beschreibung in das sogenannte Finite State Machine-Format (FSM-Format) erhalten. Dieses FSM-Format repräsentiert die zustandsendliche Beschreibung in Form sogenannter Binary Decision Diagrams (BDD), die den Vorteil besitzen, in vielen Fällen auch sehr umfangreiche Zustandssysteme kompakt zu repräsentieren. Eine Übersicht über Binary Decision Diagrams (BDD) ist in [5] beschrieben.

Ein Prozeßmodell zur Beschreibung der Reaktionen des gesteuerten Prozesses ist ergänzend zur in CSL beschriebenen Steuerungslogik erforderlich, um z.B. Aussagen über die Menge der erreichbaren Zustände zu ermöglichen. Dies kann im Rahmen des Model Checkings mit Hilfe sogenannter Assumptions, erfolgen. Da das Model Checking auch im Rahmen der formalen Verifikation der fehlerfreien Steuerung üblicherweise verwendet wird, sind diese Assumptions üblicherweise bereits vorhanden und können im Rahmen dieser Analyse erneut verwendet werden.

Mit den Assumptions wird beschrieben, wie sich die Positionen des Hubdrehtischs HD und das Vorhandensein eines Werkstücks WS in Abhängigkeit der Bewegungsrichtung und der aktuellen Position verändern können. Die unten dargestellte Assumption ('table.vmov' = stop /\ 'table.vpos' = x0) /\ x('table.vpos' = x0) stellt dar, daß, falls die vertikale Bewegung gestoppt ist und die aktuelle vertikale Position unten (x0) ist, auch im nächsten Zustand die vertikale Position x0 ist. Dieser Assumption liegt der Sachverhalt zugrunde, daß

sich Positionen nicht ändern, falls keine Bewegung stattfindet.

Im weiteren sind mögliche Assumptions, d.h. Bedingungen für die oben beschriebene Steuerung FS beschrieben:

```
process:=g ((('table.vmov' = stop  /\ 'table.vpos' = x0) /\
     /\ x('table.vpos' = x0) \/ ('table.vmov' = stop /\
     /\ 'table.vpos' = x1) /\  x('table.vpos' = x1)
     \/ ('table.vmov' = stop  /\ 'table.vpos' = x2) /\
     /\ x('table.vpos' = x2)
     \/ ('table.vmov' = plus  /\ 'table.vpos' = x0) /\
     /\ x('table.vpos' = x0 \/ 'table.vpos' = x1) \/
     \/ ('table.vmov' = plus  /\ 'table.vpos' = x1) /\
     /\ x('table.vpos' = x1 \/ 'table.vpos' = x2) \/
     \/ ('table.vmov' = plus  /\ 'table.vpos' = x2) /\
     /\ x('table.vpos' = x2) \/ ('table.vmov' = minus /\
     /\ 'table.vpos' = x0) /\  x('table.vpos' = x0) \/
     \/('table.vmov' = minus /\ 'table.vpos' = x1) /\
     /\ x('table.vpos' = x0 \/ 'table.vpos' = x1) \/
     \/ ('table.vmov' = minus /\ 'table.vpos' = x2) /\
     /\ x('table.vpos' = x1 \/ 'table.vpos' = x2)) /\
     /\ (('table.hmov' = stop  /\ 'table.hpos' = x0) /\
     /\ x('table.hpos' = x0) \/ ('table.hmov' = stop  /\
     /\ 'table.hpos' = x1) /\  x('table.hpos' = x1) \/
     \/ ('table.hmov' = stop  /\ 'table.hpos' = x2) /\
     /\ x('table.hpos' = x2) \/ ('table.hmov' = plus /\
     /\ 'table.hpos' = x0) /\  x('table.hpos' = x0 \/
     \/ 'table.hpos' = x1) \/ ('table.hmov' = plus
     /\ 'table.hpos' = x1) /\  x('table.hpos' = x1 \/
     \/ 'table.hpos' = x2) \/ ('table.hmov' = plus /\
     /\ 'table.hpos' = x2) /\  x('table.hpos' = x2) \/
     \/ ('table.hmov' = minus /\ 'table.hpos' = x0) /\
     /\ x('table.hpos' = x0) \/ ('table.hmov' = minus /\
     /\ 'table.hpos' = x1) /\  x('table.hpos' = x0 \/
     \/ 'table.hpos' = x1) \/ ('table.hmov' = minus /\
     /\ 'table.hpos' = x2) /\  x('table.hpos' = x1 \/
```

```
\/ 'table.hpos' = x2)) /\ (('table.vpos' = x0 /\
/\ 'table.hpos' = x0 /\ 'table.vmov' = stop /\
/\ 'table.hmov' = stop /\
/\ 'table.part_on_table' = nein /\
/\ x('table.part_on_table' = ja)) \/
\/ ('table.vpos' = x2 /\ 'table.hpos' = x2 /\
/\ 'table.vmov' = stop /\ 'table.hmov' = stop /\
/\ 'table.part_on_table' = ja /\
/\ x('table.part_on_table' = nein)) \/
\/ ('table.part_on_table' = ja /\
/\ x('table.part_on_table' = ja)) \/
\/ ('table.part_on_table' = nein /\
/\ x('table.part_on_table' = nein)))).
```

In Figur 8 ist ein Zustandsraum ZR des Hubdrehtischs HD und die Bewegung des fehlerfreien Hubdrehtischs HD im Zustandsraum ZR dargestellt, wie er sich nach Durchführung des Model Checkings auf die zustandsendliche Beschreibung der fehlerfreien Steuerung FS mit den angegebenen Assumptions ergibt.

In den Zeilen ist jeweils ein Wertepaar für das Tripel der Variablen (vpos, hpos, part_on_table) dargestellt. In den Spalten ist jeweils ein Wertepaar für das Tupel der Variablen (vmov, hmov) mit den jeweils oben definierten Wertemengen dargestellt.

Schraffiert Kreise in dem Zustandsraum ZR markieren hinsichtlich der Sicherheitsbedingung „verbotene" bzw. „gefährliche" Zustände. Fett markierte Kreise in dem Zustandsraum ZR markieren Zustände, die der Hubdrehtisch HD gemäß der oben angegebenen Beschreibung annehmen kann. Diese wurden durch das Model Checking ermittelt. Durch Pfeile sind Zustandsübergänge in dem Zustandsraum ZR angedeutet.

In Figur 9 ist der Zustandsraum ZR des Hubdrehtischs HD und die Bewegung des Hubdrehtischs HD im Zustandsraum ZR dargestellt, falls der Sensor 'part_on_table' fehlerhafterweise

ein Werkstück WS meldet. In Figur 9 werden die gleichen Bezeichnungen verwendet wie in Figur 8. Es ist deutlich zu erkennen, daß für diesen Fehlerfall Zustände auftreten können, die im fehlerfreien System nicht erreichbar sind. Diese Zustände sind in Figur 9 mit VZ bezeichnet.

Den einzelnen Sensoren x und/oder Aktoren y werden Ausfallwahrscheinlichkeiten zugeordnet, die jeweils die Wahrscheinlichkeit für das Auftreten eines Fehlers bei dem Sensor x bzw. Aktor y beschreiben. Durch Verknüpfung von Verbundwahrscheinlichkeiten für das Auftreten von Fehlern verschiedener Sensoren und/oder Aktoren und für das Auftreten verschiedener Zustände kann durch diese Vorgehensweise eine sehr einfach Risikoabschätzung für das technische System erfolgen. Details zur Berechnung abhängiger Wahrscheinlichkeiten in Fehlerbaäumen sind in [1] zu finden.

Somit erfolgt die Fehleranalyse unter Berücksichtigung der Ausfallwahrscheinlichkeiten.

Das Verfahren wird vorzugsweise für alle möglichen Fehler der vorhandenen Sensoren und/oder Aktoren durchgeführt.

Im Rahmen dieses Dokuments wurden folgende Veröffentlichungen zitiert:

[1] DIN 25424, Teil 1: Fehlerbaumanalyse: Methode und Bildzeichen; Teil 2: Handrechenverfahren zur Auswertung eines Fehlerbaums

[2] J. Dekleer und B. C. Williams, Diagnosing Multiple Faults, , Elsevier Science Publishers, Artificial Intelligence, Vol. 32, 1987, S. 97 -130

[3] K. Nökel, K. Winkelmann, Controller Synthesis and Verification: A Case Study, in: C. Leverentz, T. Lindner, Formal Development of Reactive Systems, Lecture Notes in Computer Science (Nr. 891), Springer 1995, S. 55 - 74

[4] J. Burch et al, Symbolic Model Checking for Sequential Circuit Verification, IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems, Vol. 13, Nr. 4, S. 401 - 424, April 1994

[5] R. Bryant, Symbolic Boolean Manipulation with Ordered Binary-Decision Diagrams, ACM Computing Survey, Vol. 24, Nr. 3, S. 293 - 318, September 1992

Patentansprüche

1. Verfahren zur rechnergestützten Fehleranalyse von Sensoren und/oder Aktoren in einem technischen System, welches in Form einer zustandsendlichen Beschreibung vorliegt, die Zustände des technischen Systems aufweist, durch einen Rechner,
a) bei dem für einen Fehler eines Sensors und/oder eines Aktors eine zustandsendliche Beschreibung des technischen Systems für den Fehlerfall ermittelt wird,
b) bei dem für das technische System eine erste Menge erreichbarer Zustände ermittelt wird,
c) bei dem für das fehlerbehaftete technische System eine zweite Menge erreichbarer Zustände ermittelt wird,
d) bei dem eine Differenzmenge aus der ersten Menge und der zweiten Menge gebildet wird,
e) bei dem Ergebniszustände aus der Differenzmenge ermittelt werden, die vorgebbaren Bedingungen genügen.

2. Verfahren nach Anspruch 1,
bei dem die Verfahrensschritte a) bis f) für alle möglichen Fehler von Sensoren und/oder Aktoren, die das technische System aufweist, durchgeführt werden.

3. Verfahren nach Anspruch 1 oder 2,
- bei dem den Sensoren und/oder Aktoren Ausfallwahrscheinlichkeiten zugeordnet werden, und
- bei dem die Fehleranalyse unter Berücksichtigung der Ausfallwahrscheinlichkeiten erfolgt.

4. Verfahren nach einem der Ansprüche 1 bis 3,
bei dem die Verfahrensschritte b) und c) nach dem Verfahren des Model Checking erfolgt.

5. Verfahren nach einem der Ansprüche 1 bis 4,
bei dem in dem Verfahren eine zustandsendliche Beschreibung eines von dem technischen System durchgeführten Prozesses berücksichtigt wird.

6. Verfahren nach einem der Ansprüche 1 bis 5,
bei dem die zustandsendliche Beschreibung durch einen endlichen Automaten realisiert wird.

7. Verfahren nach Anspruch 6,
bei dem die zustandsendliche Beschreibung durch einen endlichen Automaten in Form eines Binary Decision Diagrams (BDD) realisiert wird.

8. Verwendung des Verfahrens nach einem der Ansprüche 1 bis 7 beim Rapid Prototyping des technischen Systems.

9. Verwendung des Verfahrens nach einem der Ansprüche 1 bis 7 im Rahmen der Fehlerdiagnose des technischen Systems.

10. Verwendung des Verfahrens nach einem der Ansprüche 1 bis 7 zur Generierung kritischer Prüffälle für eine Inbetriebsetzung und einen Systemtest des technischen Systems.

11. Verwendung des Verfahrens nach einem der Ansprüche 1 bis 7 zur präventiven Wartung des technischen Systems.

FIG 1

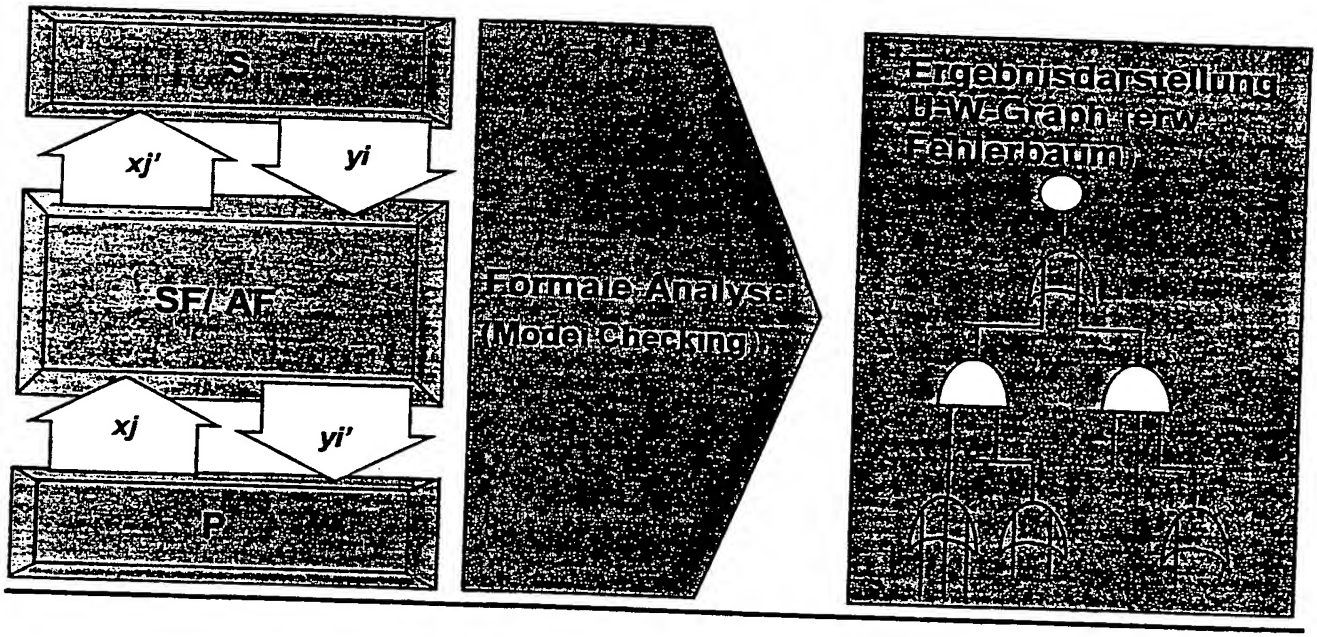


FIG 2

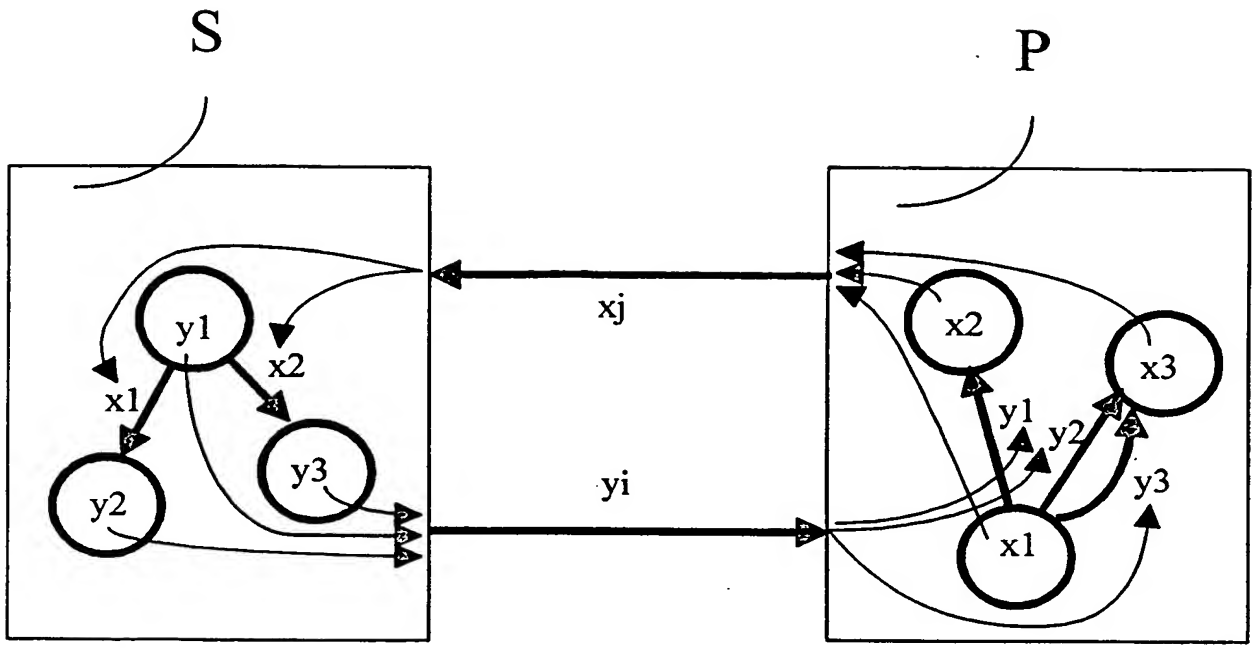


FIG 3

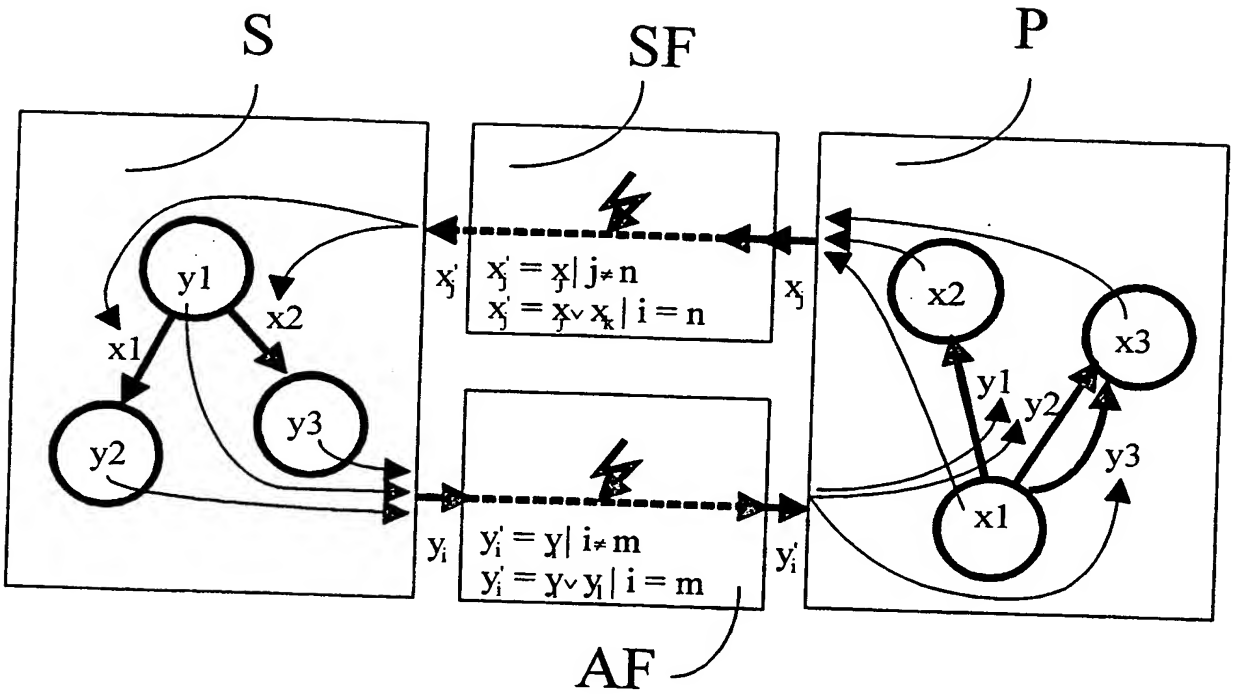


FIG 4

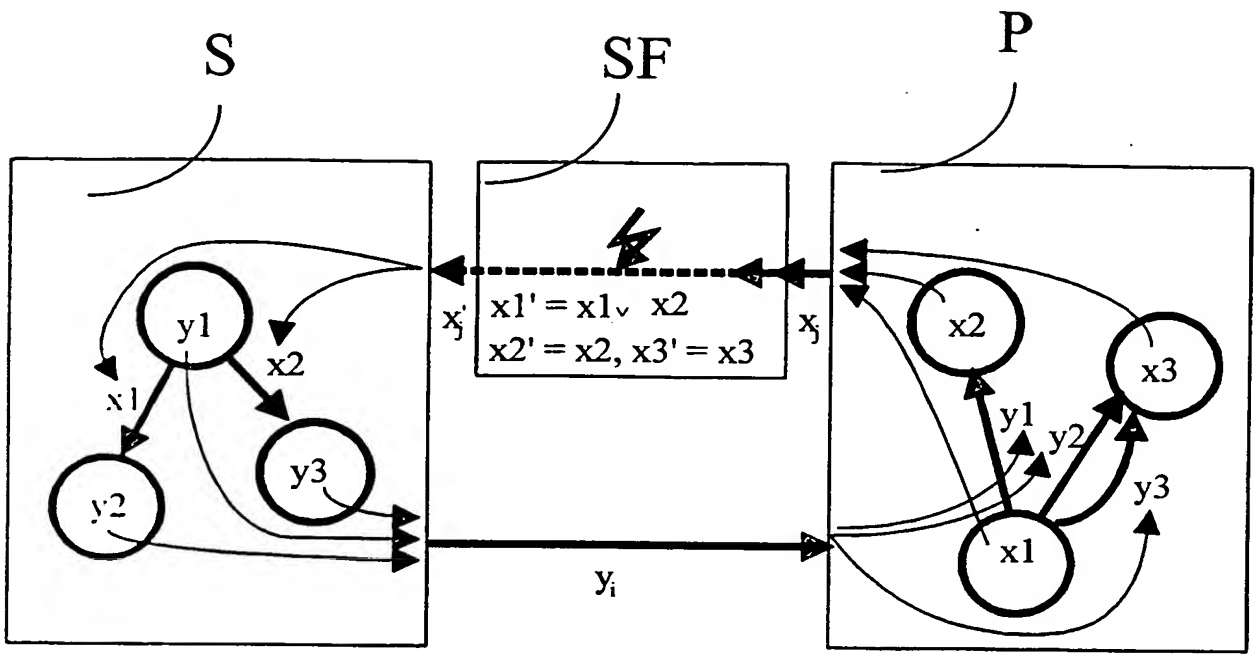


FIG 5

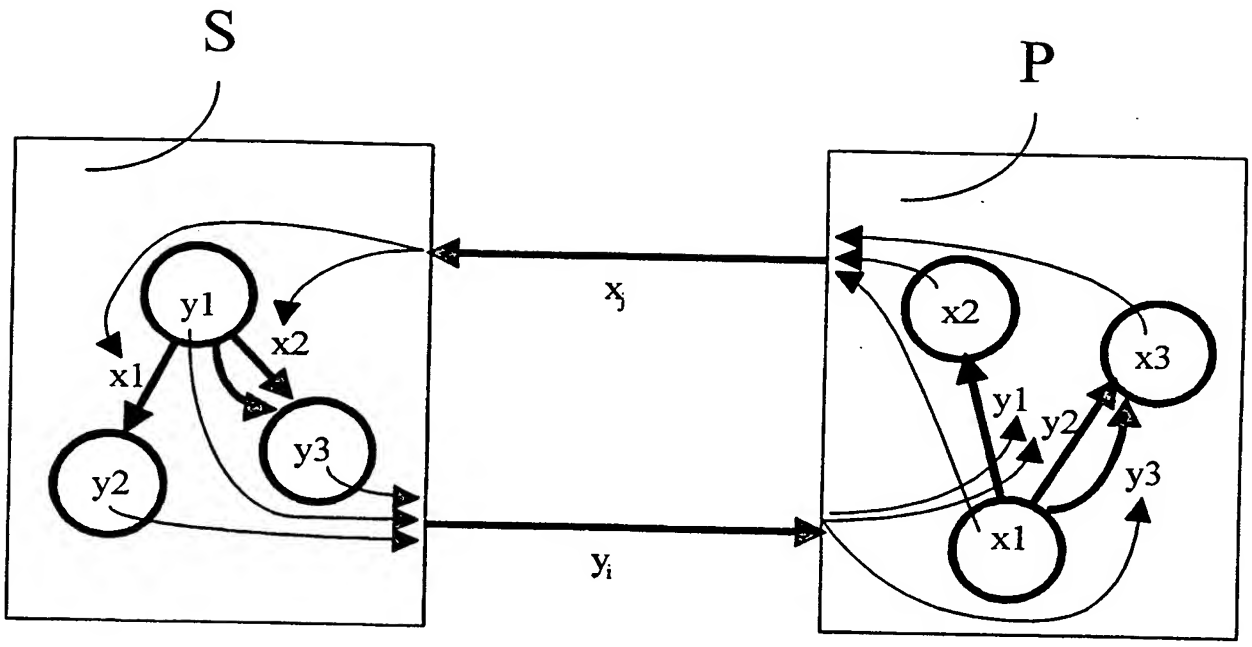


FIG 6

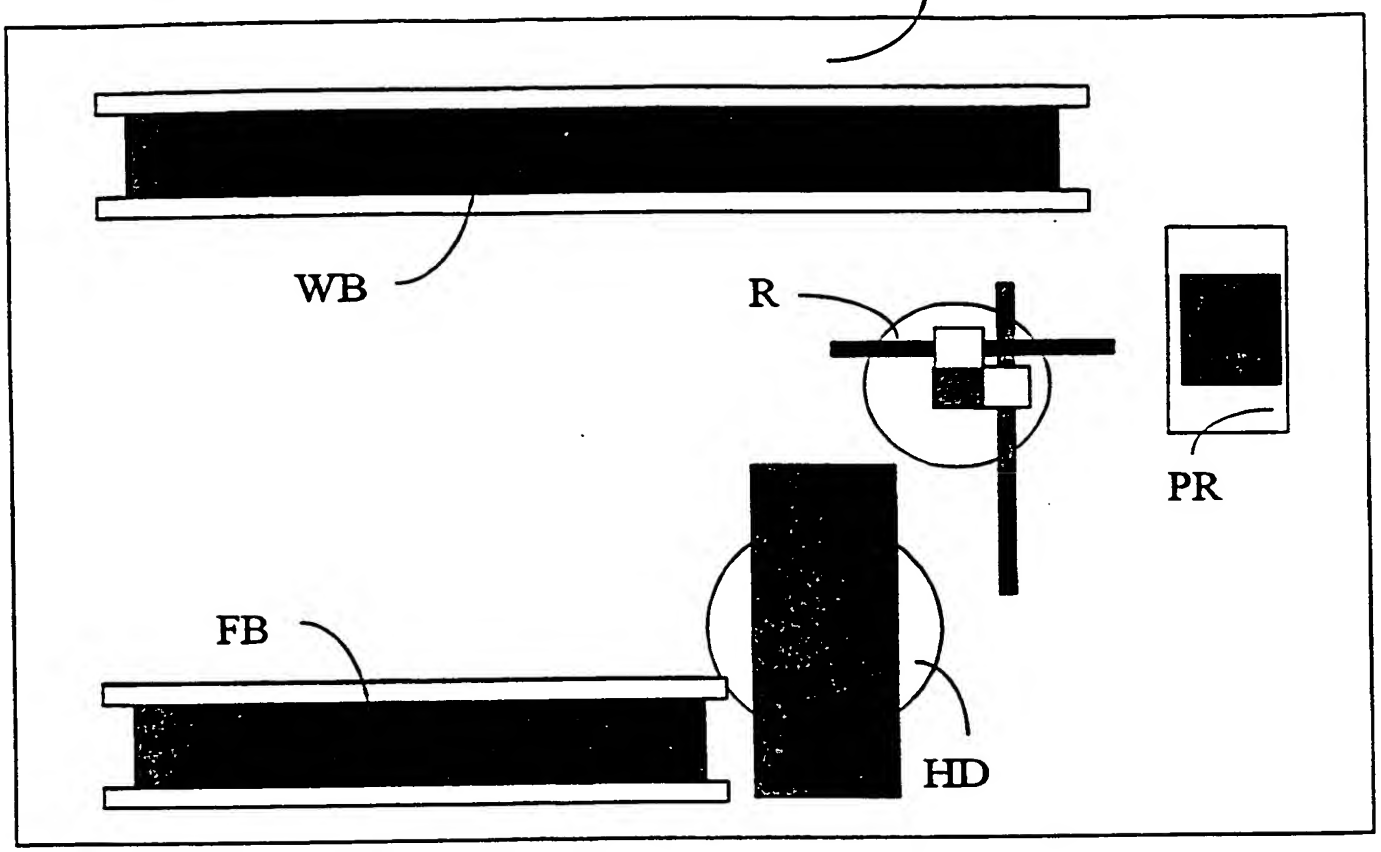


FIG 7

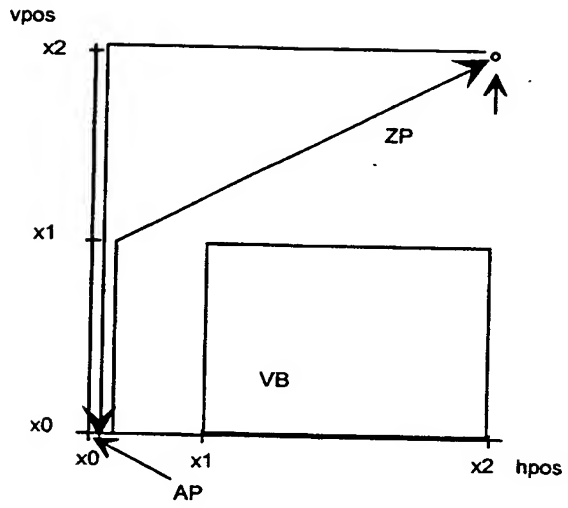


FIG 8

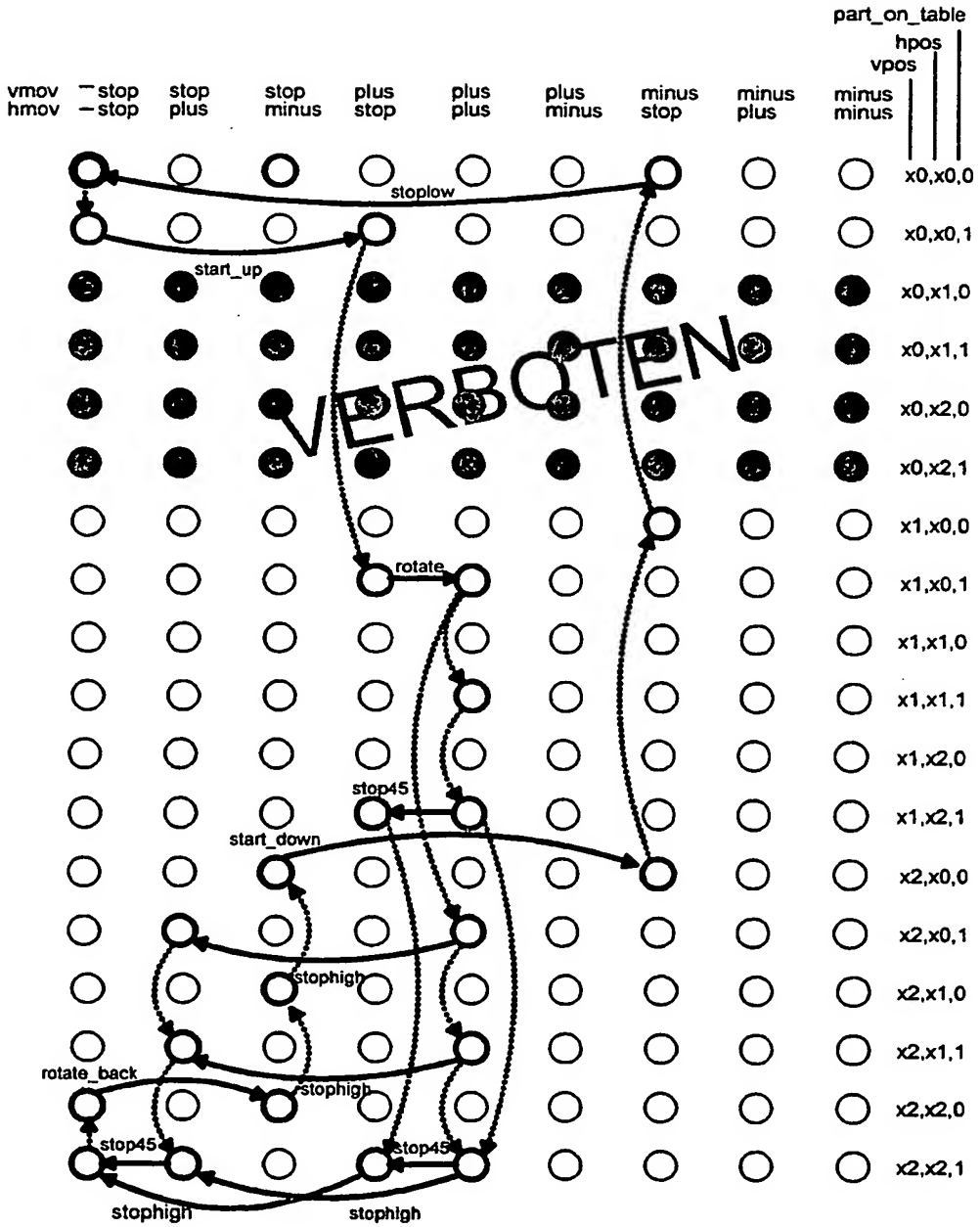
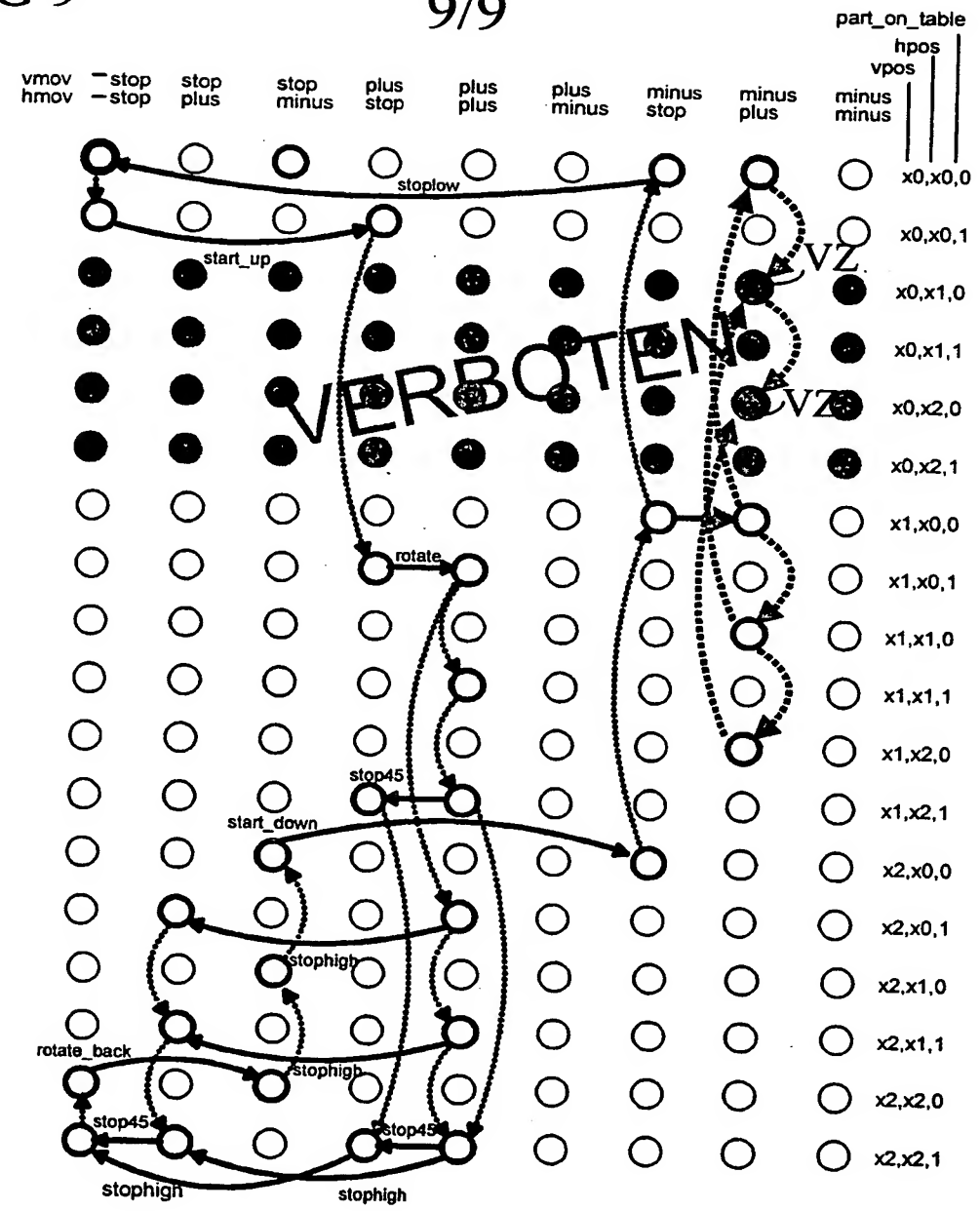


FIG 9



INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 98/00633

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G05B19/042

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 424 869 A (KOMATSU MFG CO LTD ;YAMATAKE HONEYWELL CO LTD (JP)) 2 May 1991 see column 3, line 22 - column 5, line 16; figures 1-7 ---	1-3,9
A	EP 0 352 759 B (BAYERISCHE MOTOREN WERKE AG) 17 January 1996 see column 4, line 40 - column 9, line 31; figures 1,2 --- -/--	1,2,9

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 August 1998	21/08/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Tran-Tien, T

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 98/00633

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	BURCH J R ET AL: "SYMBOLIC MODEL CHECKING FOR SEQUENTIAL CIRCUIT VERIFICATION" 1 April 1994 , IEEE TRANSACTIONS ON COMPUTER AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, VOL. 13, NR. 4, PAGE(S) 401 - 424 XP000453301 cited in the application see the whole document	1-11
A	ENDERS R ET AL: "GENERATING BDDS FOR SYMBOLIC MODEL CHECKING IN CCS" 1 January 1991 , COMPUTER AIDED VERIFICATION 3RD. AALBORG, DENMARK, JULY 1-4, 1991, PAGE(S) 203 - 213 XP000350630 see the whole document	1-7
A	EP 0 580 663 B (SIEMENS AG) 4 January 1995 see column 2, line 48 - column 11, line 25; figure 1	1,4,6
A	EP 0 685 792 A (AT & T CORP) 6 December 1995 see abstract	1,4

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/DE 98/00633

Patent document cited in search report	Publication date	Patent family member(s)	Publication dat
EP 0424869 A	02-05-1991	JP 2110034 C	21-11-1996
		JP 3137518 A	12-06-1991
		JP 8020284 B	04-03-1996
EP 0352759 B	31-01-1990	DE 3825280 A	01-02-1990
		DE 58909572 D	29-02-1996
		EP 0352759 A	31-01-1990
		ES 2081819 T	16-03-1996
		JP 2105201 A	17-04-1990
		JP 2769363 B	25-06-1998
		US 5107425 A	21-04-1992
EP 0580663 B	02-02-1994	DE 59201155 D	16-02-1995
		WO 9218944 A	29-10-1992
		EP 0580663 A	02-02-1994
		US 5491639 A	13-02-1996
EP 0685792 A	06-12-1995	CA 2147536 A	02-12-1995
		JP 7334566 A	22-12-1995
		US 5615137 A	25-03-1997

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 98/00633

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G05B19/042

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G05B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 424 869 A (KOMATSU MFG CO LTD ;YAMATAKE HONEYWELL CO LTD (JP)) 2. Mai 1991 siehe Spalte 3, Zeile 22 - Spalte 5, Zeile 16; Abbildungen 1-7 ---	1-3,9
A	EP 0 352 759 B (BAYERISCHE MOTOREN WERKE AG) 17. Januar 1996 siehe Spalte 4, Zeile 40 - Spalte 9, Zeile 31; Abbildungen 1,2 ---	1,2,9

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
17. August 1998	21/08/1998

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Tran-Tien, T

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	BURCH J R ET AL: "SYMBOLIC MODEL CHECKING FOR SEQUENTIAL CIRCUIT VERIFICATION" 1. April 1994 , IEEE TRANSACTIONS ON COMPUTER AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, VOL. 13, NR. 4, PAGE(S) 401 - 424 XP000453301 in der Anmeldung erwähnt siehe das ganze Dokument	1-11
A	ENDERS R ET AL: "GENERATING BDDS FOR SYMBOLIC MODEL CHECKING IN CCS" 1. Januar 1991 , COMPUTER AIDED VERIFICATION 3RD. AALBORG, DENMARK, JULY 1-4, 1991, PAGE(S) 203 - 213 XP000350630 siehe das ganze Dokument	1-7
A	EP 0 580 663 B (SIEMENS AG) 4. Januar 1995 siehe Spalte 2, Zeile 48 - Spalte 11, Zeile 25; Abbildung 1	1,4,6
A	EP 0 685 792 A (AT & T CORP) 6. Dezember 1995 siehe Zusammenfassung	1,4

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE 98/00633

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamili			Datum der Veröffentlichung
EP 0424869	A	02-05-1991	JP	2110034	C	21-11-1996
			JP	3137518	A	12-06-1991
			JP	8020284	B	04-03-1996
EP 0352759	B	31-01-1990	DE	3825280	A	01-02-1990
			DE	58909572	D	29-02-1996
			EP	0352759	A	31-01-1990
			ES	2081819	T	16-03-1996
			JP	2105201	A	17-04-1990
			JP	2769363	B	25-06-1998
			US	5107425	A	21-04-1992
EP 0580663	B	02-02-1994	DE	59201155	D	16-02-1995
			WO	9218944	A	29-10-1992
			EP	0580663	A	02-02-1994
			US	5491639	A	13-02-1996
EP 0685792	A	06-12-1995	CA	2147536	A	02-12-1995
			JP	7334566	A	22-12-1995
			US	5615137	A	25-03-1997